(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 May 2001 (17.05.2001)

PCT

(10) International Publication Number
WO 01/35194 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US00/30592

(22) International Filing Date:
7 November 2000 (07.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/164,673 10 November 1999 (10.11.1999) US
09/521,371 8 March 2000 (08.03.2000) US

(71) Applicant: **UNISYS CORPORATION** [US/US]; Township Line and Union Meeting Roads, P.O. Box 500, Blue Bell, PA 19424-0001 (US).

(72) Inventors: **CLAYTON, Kevin, F.**; 5 Pinewood Drive, Coto de Caza, CA 92679 (US). **DEAN, David, A.**; 60 Walden Way, Coatesville, PA 19320 (US). **KAIN, Michael, T.**; 5210 Shannon Court, Chester Springs, PA 19425-8762 (US). **SALAMON, Gary**; 812 Goshen Road D23, West Chester, PA 19380 (US). **MILLIGAN, Andrew, David**; 10 Denison Court, Wavendon Gate, Milton Keynes MK7 7JF (GB).

(74) Agents: **STARR, Mark, T.** et al.; Unisys Corporation, Township Line and Union Meeting Roads, P.O. Box 500, Blue Bell, PA 19424-0001 (US).

(81) Designated States *(national)*: AU, BR, JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR PROVIDING REDUNDANT AND RESILIENT CRYPTOGRAPHIC SERVICES

(57) Abstract: A cryptographic system (200) providing redundant and resilient cryptographic services to a computer system (120). Upon receiving a request for cryptographic services, a cryptographic services interface (207) running on a first operating environment (210) processes the request. The cryptographic services interface (207) is initialized with information specific to available operating environments (220, 230, 240) connected to the first operating environment (210) over a secure connection (124) and maintains communication protocols for various communication interfaces in the other alternate operating environments (220, 230, 240) accessible over the secure connection (124). The cryptographic services interface (207) communicates with the alternate operating environments (220, 230, 240) over communication dialogs (e.g. TCP protocol) (245, 249, 251). When processing the cryptographic service requests, the cryptographic services interface (207) facilitates the creation of cryptographic services sessions (261, 263, 265, 267) between the requestor (203, 205) and the desired cryptographic services (223, 224, 243) running on the alternate operating environments (220, 230, 240). In turn, the cryptographic services perform cryptographic functions, such as encryption, decryption, digital signing, verification, message digest creation, and random number generation on received requests. Once processed, requests are communicated back over the secure connection (124) to the requestor (203, 205) for use. The cryptographic system further monitors and stores information about the processing performed by the cryptographic services (223, 224, 243) that utilize state information when processing. Monitoring may entail processing such that if cryptographic services fail or malfunction during processing, the failed request may be re-submitted to the cryptographic services interface (207) to establish a new independent cryptographic services session (267) with cryptographic services (243) performing the same cryptographic function running on another available operating environment (240). This process allows for distributed, redundant, and resilient processing of requests for cryptographic services.

WO 01/35194 A2

METHOD AND APPARATUS FOR PROVIDING REDUNDANT AND RESILIENT CRYPTOGRAPHIC SERVICES

Field of the Invention

The present invention relates generally to providing cryptography services on a computer system, and more particularly, to providing distributed cryptographic services on a computer system having resiliency to overcome operating environment failures.

Background of the Invention

Advances in computing technologies have allowed for the development of new computing architectures that rival the performance of existing large scale computer systems and implementations (i.e. mainframe and distributive processing computing systems). The performance characteristics of new computing architectures have lent credence to a developing notion that with increasing acceptance of new computing technologies, large scale computing would realize a significant decrease in use. Contrarily, however, as information technologies have advanced, such as with the proliferation of the Internet and the World Wide Web, the developing notion has become inaccurate. Today, large scale computing is experiencing a significant resurgence. New transactional and information technologies, along with their associated software applications, require computing resources capable of performing a myriad of simultaneous transactions. Such computing needs are best suited for existing and newly developed large scale computing systems.

Along these lines, the commercial sector has capitalized on information technology breakthroughs by developing cyber-marketplaces, realms in which private and commercial consumers are afforded the ability to buy and sell goods and services using a personal computer. Corporate entities, consistent with this effort, are developing complex, robust, and efficient computer applications to reach out to their increasing customer base. As a result, the

business world is placing demands on computer manufacturers to deliver efficient, reliable, and responsive computing to support new market needs. Computer manufacturers are responding by delivering better and improved large computing architecture computer systems, that have the ability to run complex applications over multiple operating environments and different operating platforms.

With new corporate uses of computing technology comes potential hazards and concerns, such as security breaches. Hence, security is tantamount to success. Some of the information required by today's business applications can be sensitive or private in nature. By way of example, consumers participating in electronic commerce may be required to exchange private information such as credit card numbers, addresses, telephone numbers and the like. Consumers, however, would not be willing to divulge this private information without some assurance that the information proffered is to travel securely. Once again, the commercial sector has turned to computer manufacturers to develop and deliver these assurances.

Computer developers, in addressing computing security, are utilizing cryptography (i.e. process of encrypting and decrypting information passing between participating parties using a "key" known by these parties) to secure information that is exchanged. Several cryptography security standards have been developed to facilitate the exchange of information across different computing environments and operating platforms. Currently, the large computing industry appears to favor one-processor implementations of cryptographic services, which dedicates precious processing resources to one given task. In an attempt to minimize the toll on mainframe processors, some in the industry have offloaded certain cryptography services onto add-in card(s) plugged into peripheral buses, such as PCI. However, this solution can be cumbersome and may not provide fail-over resiliency in the case of a peripheral card failure. Furthermore, cryptographic services inherently demand a high and continuous level of system wide security, requiring the secured exchange of data used in cryptographic service processing.

Today, there are also large computer systems that utilize multiple operating environments. Such systems could provide efficient cryptography services by offloading

processing to available operating environments. This implementation may increase overall large computing processing efficiency and allow implementation of resiliency to accommodate fail-over processing failures. Accordingly, it is desired to provide a method and apparatus for providing distributed and resilient cryptographic services in computer systems utilizing multiple operating environments.

Summary of the Invention

The present invention provides a system and methods allowing for distributed and resilient cryptography services for a computing system. In accordance with the invention, a computer system having a plurality of independent operating environments maintains a cryptographic services interface in one of the operating environments. At least one of the other alternate operating environments maintains cryptographic services that are accessed through the interface. The cryptographic services interface also has the ability to determine which alternate operating environments are available, as well as the type and nature of any cryptographic services that might be running on such operating environments.

During operation, the cryptographic services interface initiates communication dialogs with the alternate available operating environments. Additionally, the cryptographic services interface cooperates with applications to create cryptography services processing sessions for cryptographic services processing with cryptographic services running on the alternate available operating environments. The cryptography services processing sessions operate over the established communication dialogs. The communication dialogs operate over a secure communications interface.

The cryptographic services interface receives requests for cryptographic services from local `applications` and processes such requests to establish cryptographic services processing sessions. The requests received comprise a function call to initiate cryptographic services, information or data requiring cryptography, and information about the requestor. A unique cryptographic services processing session is then created between the requesting application and a specified cryptography service found in the alternate operating environments. The cryptographic services interface facilitates the request through the established cryptographic services processing session communicating with the

required cryptographic services. In turn, the cryptographic services perform cryptographic functions on such requests and return completed requests to the cryptographic services interface, that returns them to the local applications.

During processing, the cryptographic services interface monitors and stores processing states for cryptographic services that have state information. If the distributed cryptographic services (i.e. those that are distributed into alternate operating environments) fail or malfunction during the processing of the application request, the cryptographic services interface transfers information about the failed cryptographic service processing to the requesting application. At that point, the application may resubmit an additional request to initiate a unique cryptographic services processing session. This new cryptographic services processing session may be created between the requesting application and an alternate cryptographic service, one capable of performing the desired cryptographic function.

Once processed, the cryptographic services communicate the completed requests to the cryptographic services interface. In turn, the cryptographic services interface passes the processed requests to the requesting application.

Brief Description of the Drawings

The cryptography system providing redundant and resilient cryptography in accordance with the present invention is further described with reference to the accompanying drawings in which:

Figure 1 is a system schematic of the hardware that implements the present invention;

Figure 2 is a block diagram showing the cooperation of the various operating environments in accordance with the present invention;

Figure 2A is a block diagram showing a session as contemplated by Figure 2 in accordance with the present invention;

Figure 3 is a flowchart diagram of the processing performed by the cryptographic system to initialize communication dialogs in accordance with the present invention;

Figure 4 is a flowchart diagram of the processing performed by the

cryptographic system to initialize components of the cryptographic system to receive and process requests for cryptography;

Figure 5 is a flowchart diagram of the processing performed by the cryptographic services interface when processing the requests for cryptography; and

Figure 6 is a flowchart diagram of processing undertaken by the cryptographic system when performing cryptographic functions that satisfy requests for cryptography.

Detailed Description of Preferred Embodiments

Cryptography Overview:

Data communication channels are often insecure, subjecting messages transmitted over the channels to passive and active threats. With a passive threat, an intruder intercepts messages to view the data. An effective tool for protecting messages against the active and passive threats inherent in data communications is cryptography.

Cryptography is the science of mapping readable text, called plain-text or clear-text, into an encoded and unrecognizable format, called cipher-text, and vice versa. The mapping process generally involves a series of mathematical computations on the data. The computations affect the appearance of the data, without changing its meaning.

To protect a message, an originator transforms a plain-text message into cipher-text. This process is called encryption. The cipher-text is then transmitted over the data communications channel(s). In the event that the message is intercepted, the intruder only has access to the unintelligible cipher-text. Additionally, to ensure the recipient that the true sender originated the message, and not some impostor, the sender can "digitally sign" the message with its own unique digital signature. Upon receipt, the message recipient transforms the cipher-text into its original plain-text format. This process is called decryption or decipherment. Other cryptographic primitives aside from encryption and decryption include digital signing and verification.

The mathematical operations used to map between plain-text and cipher-text are identified by cryptographic algorithms. Cryptographic algorithms require the text to be mapped, and, at a minimum, requires some value which controls the mapping process.

This value is called a key. Given the same text and the same algorithm, different keys produce different mappings. Cryptographic algorithms need not be kept secret. The success of cryptography is attributed to the difficulty of inverting an algorithm. That is, a user with the correct key can easily decrypt a message, whereas a user without a key would need to attempt random keys from a set having a myriad of possible values.

During processing, cryptographic services may employ various cryptographic algorithms. These algorithms have distinct advantages over their counterparts and may be used to satisfy different needs. For example, public key algorithms use a different key for encryption and decryption, and the decryption key cannot (practically) be derived from the encryption key. Public key methods are important because they can be used to transmit encryption keys or other data securely even when the parties have no opportunity to agree on a secret key in private. However, all known methods that utilize public key algorithms are slow, and they are usually only used to encrypt session keys (randomly generated "normal" keys), that are then used to encrypt the bulk of data using symmetric cipher (as described above). Other cryptography algorithms include secret key algorithms and cryptography hash functions.

Regardless of the algorithm employed, the goals of cryptography are to provide various services, including authentication, integrity, non-repudiation, and secrecy. Authentication allows the recipient of a message to validate its origin. It prevents an imposter from masquerading as the sender of the message. Integrity assures the recipient that the message was not modified en route. The integrity service allows the recipient to detect message modification, but not to prevent it. Non-repudiation may provide a recipient with assurance of the identity of the sender, or in the alternative, provides the sender assurance of message delivery. Secrecy, which also may be known as confidentiality, prevents the disclosure of the message to unauthorized users.

Distributed Cryptography:

In the context of computer systems and computer networks, cryptography may be implemented as a part of a computer operating environment. The computer

operating environment provides functionality dedicated to performing the complex and processing-laden cryptography computations. Furthermore, an application interface may be used to allow applications access to cryptographic functions in a standardized way. Such implementation allows multiple applications to incorporate security measures through cryptography.

By way of example, an application running in a given computer system, in accordance with the invention, may require cryptographic services as part of its functionality. The application would submit a request to the cryptographic services interface. The cryptographic services interface is first initialized such that it can communicate with the alternate operating environments running on this computer system. This communication may be realized through the creation of communication dialogs (e.g. using the TCP/IP protocol) over a secure communication interface. As part of the initialization, the application interface recognizes available alternate operating environments that have cryptographic services and the nature of the cryptographic services. The cryptographic services provide a library of routines that perform various functions including, encryption, decryption, and digital signatures. After initialization and upon receiving a request for a specific cryptographic service, the cryptographic services interface initiates cryptographic services processing sessions between the requestors and the desired cryptographic services found in the alternate operating environments. The sessions are used to distribute requests for specific cryptographic functions, for example such as a request for encryption or decryption, to those cryptographic services capable of performing the desired function.

When receiving a cryptographic services request, the cryptographic services inter- face processes the request and attempts to create a session between the requestor and the desired cryptographic service using the established communication dialogs. As the session is independent of the communication dialog, the cryptographic services interface can process a number of requests simultaneously over the established communication dialogs operating between the cryptographic services interface and cryptographic services foundin available alternate operating environments. The request is processed by the cryptographic services and then passed back to the application through the cryptographic services interface for use.

Additionally, the cryptographic services interface monitors and stores processing states about specific cryptographic services that have state information. The monitoring is performed to provide resiliency for applications requesting such cryptographic services. That is, the cryptographic services interface is monitoring for faulty or incomplete processing. In the event of incomplete or faulty processing, the cryptographic services interface communicates information about the failed cryptographic service to the requesting application. The application may then resubmit the failed cryptographic processing request with this state information to the cryptographic services interface to establish a different unique cryptographic session. This session may be established with a cryptographic service performing the same cryptographic function, but running on yet another alternate operating environment. The new session, like its predecessor, operates over the communication dialogs established between the cryptographic services interface and the alternate operating environment. By doing so, the cryptographic services interface provides fail-over protection.

However, there are potential hazards for using cryptographic functions in the computerized network setting. Since the functions are carried out electronically, the user might assume the cryptographic routines are operating as expected, yet not be aware of sophisticated electronic attacks. Careless applications might use cryptographic encryption or signature keys in ways to jeopardize the keys' secrecy. Moreover, malicious applications might even deliberately compromise the user's secrecy, or worse, perform unauthorized cryptographic operations. For instance, a malicious application, might attempt to decrypt the user's secret files and transmit them to some adverse party. Another situation might involve an application attempting to digitally sign information on behalf of a user without the user's knowledge or consent. A computer implemented cryptographic system must therefore provide the needed security to prevent attack from poorly devised or malicious applications.

There are several countermeasures that may be implemented to overcome security problems inherent in computer networks. For example, the computer network may be designed such that the network connections are physically proximate to each other. By doing so, the computer network may be more easily monitored for

unwarranted or unsolicited activities.

In the case described above, the present invention may be utilized to realize cryptography. The present invention contemplates a method and apparatus for providing cryptography services to applications wherein the processing for the cryptography is distributed among independent operating environments that cooperate through an electronic connection. However, as described above, in order for cryptography to be successful, the processing for cryptography should be secure. Accordingly, the present invention requires a secure electronic connection between the cooperating independent operating environments for proper operation. The secure connection is needed so that cryptographic processing is not compromised.

Security may be accomplished by providing a monitored physical connection between the various network hardware running the computer operating environments. This type of security may be ensured by keeping the network hardware in close proximity to each other. Alternatively, in the case where all of the computer operating environments reside and run in a single computer hardware configuration, the connection may be secured through software to secure communications between the computer operating environments.

A preferred secure communication scheme is one that facilitates secure communication among heterogeneous computer systems having varying hardware configurations and running varying operating environments. Example implementations of such secure communication schemes are Virtual Transport Layers using a Messaging SubSystem (VTL/MSS) and Virtual LANs (VLANs). Generally, MSS is a system interconnect independent messaging transport which presents to its users many different delivery and notification mechanisms for the transfer of both control and data information between different heterogeneous environments, while VTL uses the MSS connection to provide a consistent, interconnect independent interface. Comparatively, a VLAN enables a first network protocol provider, executing on a first computer system, and second network protocol provider , executing on a second computer system which is directly interconnected to the first computer system, to communicate at high speed, with low latency, such that both systems may use their native mechanisms to communicate with each other without change in those mechanisms, rather than over

conventional communication paths. As such, these communication schemes allow heterogeneous computer systems to communicate without sacrificing security. Virtual transport layers (VTLs) and Virtual LANs (VLANs) are proposed in pending U.S. Patent Applications Serial No. 09/126,920 and Serial No. 09/088,552, respectively. These applications are assigned to the present assignee and the contents thereof are hereby incorporated by reference in their entirety.

As will be described below with respect to Figures 1-6, the present invention is directed to a system and methods providing distributed and resilient cryptographic services for a computer system. In accordance with a preferred embodiment thereof, the present invention comprises a system and method to distribute cryptographic service processing among a plurality of computing operating environments capable of performing cryptographic processing and to monitor these computer operating environments such that if a computing environment fails during cryptographic service processing, the request (if desired) can be redistributed to an alternative computer operating environment having the required cryptographic service.

In one embodiment, described more fully hereinafter, the methods and apparatus of the present invention may be implemented as part of a computer system having a plurality of computer operating environments. Although the depicted embodiment provides distributed and resilient cryptography for a computer system having operating environments residing in disparate computing hardware, those skilled in the art will appreciate that the inventive concepts described herein extend to various types of computer system configurations having a plurality of computing operating environments running on various hardware configurations.

System Overview:

Figure 1 shows a stand-alone computer 100 communicating with computer system 120 over computing network 110. As shown, computing system 120 includes a plurality of computing devices 122, 125, 126, and 127. Computing device 122 (which may take the form of a large scale computer such as a mainframe) communicates with alternate computing devices 125, 126, and 127 (that may take the form of computer servers) through secure communication interface 124. During operation, an operator

(not shown) may request and transmit information through computer 100 to and from computing system 120 over computing network 110. This information may be part of an application (such as an e-commerce application) (not shown) or application protocol operating between computer 100 and computing system 120. Additionally, this information may be sensitive and require cryptographic services. When cryptography services are required from computing system 120, computing system 120 processes the request and performs cryptographic services on a cryptographic service system (as shown in Figures 2 and 2a) in accordance with the request. In an illustrative embodiment, computing system 120 is a UNISYS MCP running on a CLEARPATH HMP/NX mainframe computer system, and computing devices 125, 126, and 127 are WINDOWS NT servers, running on INTEL processors.

Figures and 2 and 2a show a cryptographic system 200 of the present invention. As indicated in Figure 2, cryptographic system 200 is typically based on some form of computer or computer system. The type of computer or computer system is not important and could be a personal computer, a mainframe system, or some intermediate machine.

Cryptographic system 200 has a plurality of computing operating environments 210, 220, 230, and 240. Further, Figure 2 shows operating environment Alpha 210 maintaining computing application A 203 and computing application B 205. Applications 203 and 205 are linked to cryptographic services interface 207 of operating environment 210. Cryptographic services interface 207, in turn, is electronically coupled to a plurality of operating environments 220, 230, and 240 through communication interface 124 (of Figure1). Similarly, operating environments 220, 230, and 240 maintain cryptography services processing interfaces 221, 231, and 241, respectively. These cryptography services processing interfaces 221, 231, and 241cooperate with cryptographic services interface 207 to communicate information between the applications 203 and 205 of operating environment 210, and cryptographic services 223, 224, 233, 243 of operating environments 220, 230, and 240, respectively. This communication of information is facilitated through the use of communication dialogs 245, 249, and 251 and procedure calls 253, 255, 257, and 259. In turn, each of the

cryptographic services 223, 224, 233, and 243 performs one or more of the various functions required for cryptography.

During initialization of operating environment 210, cryptographic services processing interface 207 determines which alternate operating environments are available and proceeds to initiate communication dialogs (e.g. TCP/IP dialogs) over secure communication interface 124, with cryptography services interfaces 221, 231, and 241 of alternate operating environments 220, 230, and 240. In using communication dialogs 245, 249 and 251, cryptographic service interface 207 is capable of determining any changes to the operation of already detected and cooperating alternate operating environments or to detect the presence of newly instituted operating environments.

As part of communication dialog initialization, cryptographic service interface 207 determines which cryptographic services are available, as well as the type of cryptographic functions these services may perform. For example as shown in Figure 2, operating environment beta 220 maintains cryptographic service A 223 and cryptographic service B 224. Cryptographic service A 223 may perform a given set of cryptographic functions that are different from the cryptographic functions performed by cryptographic service B 224. Further, as Figure 2 shows, the cryptographic services have particular configuration requirements. That is, multiple occurrences of a given type of cryptographic service (i.e. cryptographic service A, B, or C) may reside among the many alternate operating environments 220, 230, and 240, but only a single occurrence of a cryptographic service type (i.e. cryptographic service A, B, or C) can reside within a given alternate operating environment. Once established, communication dialogs 245, 249, and 251 may be used by computing applications 203 and 205 when requesting cryptographic services.

In operation, an operator through an application or application protocol may request services from computing application 203 or computing application 205 residing in operating environment 210. As part of this request, computing application 203 may be required to communicate information using some form of cryptography. In an effort to satisfy the request, computing application 203 may submit a request for cryptographic

services requiring specific cryptography functions (e.g. such as encryption) for some given information to cryptographic services interface 207. As shown in Figure 2a, upon receiving a request for cryptography, cryptographic services interface 207 establishes one of the independent sessions 261, 263, and 265 between the requesting application 203 or 205 and the targeted cryptographic services 223, 224, 233, and 243 (depending on what the requesting application needs). In turn, cryptographic services 223, 224, 233, and 243 perform various cryptography functions (e.g. encryption, decryption, or digital signatures) in the effort to satisfy the request. Additionally, during cryptographic services processing (i.e. when performing cryptographic functions), cryptographic services interface 207 may monitor and store information about such processing.

As shown in Figure 2, application A 203 and application B 205 may communicate with cryptographic services interface 207 through procedure calls 225, 227 and 229. Such procedure calls facilitate the creation of independent cryptographic processing sessions. In the creation of such sessions, cryptography state information about the cryptographic service request and subsequent cryptographic services 223, 224, 233, and 243 processing may be stored by both applications 203 and 205 and cryptographic services interface 207. Indicated in Figure 2, cryptography processing variable states α 213, 215, and 217 are maintained by applications 203 and 205 and cryptography states-stores β 213', 215', and 217' are maintained by cryptographic services interface 207. The cryptography processing variable states α 213, 215, and 217 and cryptography states-stores β 213', 215' and 217' are communicated to and from the cryptographic services interface 207 during cryptographic services request processing. The state information will generally be stored for cryptographic services requests and cryptographic services processing that require state information for proper operation (e.g. cipher chain block (CBC) encryption).

Each session 261, 263, 265 or 267, as shown in Figure 2a, is initiated such that the session is in communication with only one specific cryptographic service. Hence, if a request is made by application A 203 for encryption, cryptographic services interface 207 will initiate a session over an established communication dialog (e.g. 245) between application A 203 and the cryptographic service capable of performing the requested encryption (e.g. cryptographic services B 224). In the event that application B 205

requests the same cryptographic service (e.g. cryptographic services B 224) for which a session has been established with application A, cryptographic services interface 207 creates an independent session, regardless of the already established cryptographic services session, between application B 205 and the desired same cryptographic service (i.e. cryptographic services B 224).

Communications offered by cryptographic services interface 207 that are directed towards cryptography are received by cryptography processing interfaces 221, 231, and 241 of operating environments 220, 230, and 240, respectively. Cryptography processing interfaces 221, 231, and 241 communicate with cryptography services 223, 224, 233, and 243 to pass the various requests for cryptography. In turn, cryptographic services 223, 224, 233, and 243, each having the ability to independently perform various cryptographic functions, performs requested cryptography functions on the passed information. Cryptography services 223, 224, 233, and 243 pass back cryptography processed information to cryptography services processing interfaces 221, 231, and 241. The cryptographic processed information in turn is passed back to cryptographic services interface 207. Cryptographic services interface 207 passes the cryptographic processed information to application 203 for use. Application 203 or 205 is now capable of providing the requested information to the originator of the request.

Cryptographic services interface 207 also maintains monitoring and storage features such that it monitors and stores information about the processing performed by certain cryptographic services 223, 224, 233, and 243 for submitted requests. Monitoring and storage features are generally performed by cryptographic services interface 207 for cryptographic services that require cryptography state information to perform cryptographic processing (e.g. CBC encryption or decryption). When this specific kind of cryptography service fails or malfunctions, the cryptographic service will pass information about the state of the failed processing back to cryptographic service interface 207 through communication dialogs 245, 249, or 251. The cryptography state information is stored in cryptography states-stores β 213', 215', or 217' of cryptographic services interface 207 and forwarded to cryptography processing variable states 213, 215, or 217. The original requestor is notified of the failed cryptographic processing and is passed the failed processing state information generated by this

specific kind of cryptographic services 223, 224, 233, and 244. Using this information about failed cryptographic services processing, the original requestor may choose to re-submit the failed cryptographic services request to cryptographic services interface 207 for processing. The request along with the failed state processing information is processed by cryptographic services interface 207 to find an appropriate alternate cryptographic service 223, 224, 233 or 243 (i.e. a cryptographic service that performs the same cryptographic functions and that use state information when performing cryptographic functions) running on an alternate operating environment to satisfy the request. If an appropriate alternate cryptographic service is found, the failed request is used to create a new independent cryptographic services processing session between the requesting application 203 or 205 and the newly discovered appropriate alternate available cryptographic service.

The new independent session uses the stored failed processing cryptography state information to realize cryptographic services processing. Specifically, the cryptographic services associated with the alternate session uses the failed processing state information from the previous cryptographic services processing attempt to perform cryptographic services on the re-submitted request. In the event that there are no available appropriate alternate cryptographic services, cryptographic service processing is suspended by the application for the re-submitted request until an appropriate alternate session is established.

For example, as shown by Figures 2 and 2a if a request is being processed by cryptographic services B 224 in session 263 fails during processing, cryptographic services interface 207 would receive information about the failed processing from cryptographic services 221 and notify the original requestor (e.g. application 203) about the failed processing, including communicating the failed processing state information. If the original requestor re-submits the request (i.e. a request for cryptographic services that perform cryptographic functions like cryptographic services B 224), the request is used to create a new independent session (e.g. cryptographic services session 267 operating over communication dialog 227') with a cryptographic service on another alternate operating environment (e.g. operating environment theta 240) performing the same cryptographic function (e.g. cryptographic service B 243 of operating environment

240) that previously failed.

Cryptographic system 200 now will be described by way of example. A customer may want to purchase a product over the Internet (e.g. via the World Wide Web).

Accordingly, a customer may browse a retailer's web-site that house information about various products and services. In addition, the customer may purchase or place an order for a product or service on the retailer's web-site that may have an application dedicated to customer order placement and processing. This application may be considered the exemplary computing application 203 or 205 of Figure 2. As part of order processing, sensitive information may be transferred between the customer and the retailer (e.g. payment information, delivery information, confirmation numbers and the like), and may require cryptography.

The application described may reside on the retailer's computing system. Furthermore, the retailer's computer system may be capable of running a plurality of operating environments of varying platforms. Additionally, the information transferred to the retailer's application may have been locally processed for cryptography on the customer's computer, such that when the customer transfers information to the e-commerce application such information is already processed in the cryptography format. The application 203 would thus be required to process this cryptographic formatted information. As such, application 203 calls upon the cryptographic services interface 207, placing a request for cryptographic services. The cryptographic services interface 207 is initialized such that it is aware of the available cryptographic services running in the various operating environments of the retailer's computer system. In addition, the cryptographic services interface 207 facilitates the creation of cryptographic services sessions (e.g. cryptographic sessions 261 and 263 operating over communication dialogs 225 and 227, respectively) between a requesting application 203 or application protocol and available cryptographic services 223, 224, 233, and 243 found in alternate independent operating environments. The cryptographic service communicates to the cryptographic services of the alternate operating environments through communication dialogs that operate over a secure communication interface. Such

communication dialogs work on accepted communication standards and protocols (e.g. TCP/IP.) In operation, the cryptographic services interface 207 receives requests form a computing application or application protocol and helps to create cryptographic services sessions between the requestor (i.e. computing application) and the available and desired cryptographic services running on the alternate operating environments. The information is processed by the cryptographic services and returned to the e-commerce application for use.

If the cryptographic services fail during processing, cryptographic services interface 207 may communicate state information, that it may have stored, about the failed cryptographic processing back to the requestor (e.g. e-commerce application.) The requestor may re-submit the request for the same cryptographic services processing to the cryptographic services interface. The cryptographic service interface may then look for an appropriate alternate cryptographic service (i.e. a cryptographic service performing the same cryptographic function that failed) running on an alternate operating environment to satisfy the re-submitted request.

Additionally, there may be another computing application 205 (e.g. a secure corporate intranet) running on the same operating environment that may require the same cryptographic services that are employed by the e-commerce computing application 203. Since the sessions are independent of each other, when the secure corporate intranet application sends a request for the same cryptographic service to the cryptographic services interface 207, the cryptographic services interface 207 creates a new and independent cryptographic services session (e.g. 265) between the secure corporate intranet computing application and the desired cryptographic service (e.g. cryptographic services B 224.) As Figures 2 and 2a illustrate, the new independent cryptographic service session (e.g. session 265) may operate over the same communication dialog (e.g. communication dialog 245) but does not interact with the existing cryptographic services session that exists between the e-commerce application and cryptographic services (e.g. session 263). Hence, the cryptographic services interface 207 may serve to multiplex sessions over the same communication dialog between requesting applications and desired cryptographic services.

Figures 3-5 describe the processing performed by cryptographic system 200 of Figure 2. Figure 3 shows the processing performed by the cryptographic services interface 207 when initializing communication dialogs (e.g. TCP/IP protocols) between itself and alternate operating environments 220, 230, and 240. Communication dialog initialization processing starts at block 300 and proceeds to block 305 where the cryptographic services interface 207 is initialized as operating environment alpha 210 is initialized. Processing proceeds to block 310 where a list of active operating environments is received by the cryptographic services interface 207 from the secure interconnect. The cryptographic services interface 207 then selects the first (or next) active operating environment from the list at block 315. A check is then made at block 320 by the cryptographic services interface to determine if there are any more active environments on the list. If there are no more active operating environments to accept, communication dialog initialization processing ends at block 325 as the cryptographic services interface 207 is now ready to accept requests to establish cryptographic services sessions.

However, if at block 320 there are additional operating environments, the cryptographic services interface 207 proceeds to establish a secure communication dialog at block 330 with the complimentary cryptography services interface (e.g. 221, 231, or 241) in the recognized active operating environment. A check is then made by the cryptographic services interface 207 at block 335 to determine if the communication dialog was successfully established. If the communication dialog was successfully established, the operating environment with which the communication dialog was successfully established is marked by the cryptographic services interface 207 at block 345 as being ready to process cryptography requests. Processing reverts to block 315 and proceeds therefrom. In the event that the communication dialog was not successfully established with the targeted active operating environment at block 330, the operating environment is marked as being not ready by the cryptographic services interface 207 at block 340. Processing then reverts to block 315 and proceeds therefrom.

Figure 4 shows the processing performed by cryptographic system 200 when cryptographic services are requested. As described by Figure 3, operating environments

210, 220, 230, 240, cryptographic services interface 207, and cryptography processing interfaces 221, 231, and 241 are initialized. The initialization process ensures that secure communication interface 124 is working properly and establishes basic components of communication protocols between cryptographic services interface 207 and cryptography processing interfaces 221, 231, and 241. The initialization of the cryptographic system 200 having been completed, cryptographic system 200 is now ready to provide cryptographic services.

Figure 4 shows that at block 410, a local application requests a cryptographic session to a cryptographic service. At block 411, the list of cryptographic services produced by cryptographic services interface 207 of available alternate operating environments is checked, and if the requested service is available, then a cryptographic services session is established by the cryptographic services interface 207 for the local application at block 420. The cryptographic services interface 207 subsequently notifies the requestor at block 425. The application is now ready to initialize the session for a specific cryptographic function at block 429. If at the time, in block 411, the requested cryptographic service is not available, then cryptographic services interface 207 notifies the requestor that the requested cryptographic service is not available at block 415, and processing ends at block 430.

Figure 5 shows the processing that cryptographic services interface 207 performs when cryptographic services interface 207 is requested to initialize a specific cryptographic function for an established cryptographic session. The request to initialize a specific cryptographic function for a specific cryptographic service, for example, encryption, is received from the local application (i.e. 203) by cryptographic services interface 207 at block 501. The cryptographic services interface 207 sends the initialization request to the service associated with the user session at block 505. The cryptographic services interface 207 then monitors and stores information about the cryptographic processing in alternate environments at block 510. At block 520, the completion of the initialization request is made. If the processing completed successfully, then the local application (the requestor) is notified that his request completed successfully at block 527, and that further requests can be made through this session. Processing then terminates at block 529, and the application is ready to request

a cryptographic function. If the processing did not complete successfully at block 520, the requestor (the local application) is notified at block 525, and processing for this request terminates at block 530. The application is ready to destroy the cryptographic session.

Figure 6 shows the cryptographic services interface 207 processing a user request for a cryptographic function. The request is sent to the cryptographic services interface 207 at block 601. At block 605, the cryptographic services interfaces 207 sends the request to the cryptographic services in the alternate operating environment associated with the user session. The cryptographic services interface 207 then monitors and stores information about the alternate operating environments at block 610. The cryptographic services interface 207 then checks to see if the request completed successfully at block 620. If the alternate operating environment failed, or the request was not completed successfully, the cryptographic services interface 207 notifies the requestor of the failure at block 621 and terminates the cryptographic session. At this time, the local application can request a new cryptographic session at block 655, if it so desires, and processing would then revert to block 410 of Figure 4. If the request completed successfully, the cryptographic services interface 207 receives the completed request and any residual state information from the alternate operating environment that performed the request at block 625. This information is returned to the requestor (the local application 203) at block 630. A check is then made at block 640 to determine if more information is required when performing the cryptography function. If there is more processing necessary for this cryptographic function (some cryptographic functions require more than one iteration), then processing goes back to step 605, and proceeds through until the entire function request has been satisfied. When no more processing is required, flow proceeds to step 650. If the requestor needs another cryptographic function, flow proceeds to step 501 of Figure 5. If the requestor does not need another function, then the cryptographic session terminates, and processing ends at block 665.

In sum, the present invention provides a system and process for providing redundant and resilient cryptography on a computer system. It is understood, however, that the invention is susceptible to various modifications and alternative constructions.

There is no intention to limit the invention to the specific constructions described herein. On the contrary, the invention is intended to cover all modifications, alternative constructions, and equivalents falling within the scope and spirit of the invention.

For example, the present invention may be implemented in a variety of computer systems. The various techniques described herein may be implemented in hardware or software, or a combination of both. Preferably, the techniques are implemented in computer programs executing on programmable computers that each include a processor, a storage medium readable by the processor (including volatile and non-volatile memory and/or storage elements), at least one input device, and at least one output device. Program code is applied to data entered using the input device to perform the functions described above and to generate output information. The output information is applied to one or more output devices. Each program is preferably implemented in a high level procedural or object oriented programming language to communicate with a computer system. However, the programs can be implemented in assembly or machine language, if desired. In any case, the language may be a compiled or interpreted language. Each such computer program is preferably stored on a storage medium or device (e.g., ROM or magnetic disk) that is readable by a general or special purpose programmable computer for configuring and operating the computer when the storage medium or device is read by the computer to perform the procedures described above. The system may also be considered to be implemented as a computer-readable storage medium, configured with a computer program, where the storage medium so configured causes a computer to operate in a specific and predefined manner.

Although exemplary embodiments of the invention has been described in detail above, those skilled in the art will readily appreciate that many additional modifications are possible in the exemplary embodiments without materially departing from the novel teachings and advantages of the invention. Accordingly, these and all such modifications are intended to be included within the scope of this invention as defined in the following claims.

WHAT IS CLAIMED IS:

1. A system (200) for providing cryptographic services on a computing system (120) having a plurality of independent operating environments (210, 220, 230, 240), comprising:

at least one cryptographic service (223) running in a first operating environment (220);

a secure communications interface (124) which couples said plurality of operating environments (210, 220, 230, 240) such that said first operating environment may transfer to and receive electronic information from others of said plurality of operating environments (210); and

a cryptographic services interface (207) residing in a second operating environment (210) working in conjunction with said first operating environment (220) such that said second operating environment (210) may transfer and receive cryptographic service processes from a computing application (203, 205) local to said second operating environment (210).

2. The system recited in claim 1, wherein said cryptographic services interface establishes and initializes communication dialogs operating on said secure communications interface to communicate said cryptographic services processing information, said cryptographic services interface monitoring said plurality of operating environments for availability of cryptographic services, and communicating and distributing said cryptographic service process information to available cryptographic services running in at least one of said plurality of operating environments through said secure communications interface, said cryptographic services receiving said cryptographic service process information, performing cryptographic processing on said information, and returning cryptographic processed information through said secure communications interface to said application submitting said requests.

3. The system recited in claim 2, wherein said cryptographic services interface facilitates the creation of cryptographic services sessions between said requesting computing application and said cryptographic services running on said alternate

operating environments that perform cryptographic functions.

4. The system recited in claim 2, wherein said communication dialogs comprise TCP/IP protocols and standards.

5. The system recited in claim 2, wherein said available cryptographic services comprise cryptographic services that utilize and store processing state information during operation.

6. The system recited in claim 5, wherein said cryptographic services interface further monitors said available cryptographic services during cryptographic service processing such that if a cryptographic service fails during cryptographic service processing of cryptographic service process information said cryptographic services interface determines if alternate cryptographic services are available for processing said cryptographic service process information.

7. A method for providing distributed and resilient cryptographic services on a computer system (120), comprising the steps of:

(a) creating at least one secure cryptographic services session (261) between a first operating environment (210) and a second operating environment (220), wherein said session (261) operates between components (207) of said first operating system (210) and components (221) of said second operating system (220), said session (261) processes requests by said components for cryptographic services, said request containing information or data needing cryptography;

(b) determining available and appropriate cryptographic services (223, 224, 243) to perform cryptographic service processing to satisfy said request;

(c) storing information about available cryptographic services; and

(d) routing said request to available cryptographic services (223) through said session (261) wherein said cryptographic services perform cryptographic functions on said request.

8. The method recited in claim 7, further comprising the steps of:

(a) monitoring processing state information about said cryptographic services and storing and monitoring said processing state information about cryptographic services processing; and

(b) processing said monitoring information such that if cryptographic services fail during processing, said processing state information is passed to said component originating said cryptographic services request, said component re-submitting said request to create a new and independent cryptographic services session between said component and available appropriate cryptographic service using said processing state information.

9. The method recited in claim 7, wherein said request is offered by a computing application running on one of a plurality of operating environments cooperating with other computer systems through various communication interfaces, including the Internet.

10. In a computer system (120) running a plurality of computer operating environments (210, 220, 230, 240), a method for supporting cryptographic functions, the method comprising the steps of:

(a) supplying a request for a cryptographic function to a cryptographic services interface (207), said request containing information or data needing cryptography;

(b) creating at least one secure cryptographic services session (261) upon receiving said request, wherein said session (261) provides a first operating environment (210) access to specific cryptographic service processing found in a second operating environment (220);

(c) determining available operating environments (220, 230, 240) running cryptographic services (223, 224, 233, 243);

(d) establishing communications with at least one available operating environment;

(e) processing said request received by said cryptographic services interface (207) through said session (261) to said available operating environment (220) running cryptographic services (223); and

(f) performing cryptographic functions in said available operating environment.

11. .The method recited in claim 10, further comprising the steps of: monitoring and storing information about cryptographic processing performed in said available operating environment and, if said cryptographic service fails during processing, using said stored information about cryptographic processing performed to facilitate the creation of a new independent cryptographic services session to process said failed request to another available appropriate cryptographic service.

12. A method as recited in claim 10 wherein the step (f) comprises performing a cryptographic function selected from a group comprising encryption, decryption, digital signing, verification, message digest creation, and random number generation.

13. In a computing system having a mainframe computer running a first operating environment and a plurality of computer servers running operating environments different from said first operating environment, a system to provide cryptography comprising:

a first cryptographic services interface running in said first operating environment accepting requests from applications local to said first operating environment to perform cryptographic services;

a second cryptographic services interface running in a second environment on one of said computer servers and cooperating with said first cryptographic services interface to receive and process said requests, wherein said second cryptographic services interface communicates over a secure communications interface with an operating environment running on said one computer server to distribute requests received from said first operating environment to said second operating environment; and

at least one cryptographic service running in said second operating environment, capable of performing cryptographic functions on received requests, wherein said cryptographic services are coupled to said second cryptographic services interface and said second cryptographic services interface acts to communicate with said first

cryptographic services interface to receive requests for cryptographic processing and pass back processed requests.

14. The cryptographic system recited in claim 13, wherein said first cryptographic services interface monitors and stores information about requests from the time of the initial request to when said request has been processed for cryptographic services and passed back to said local applications, wherein said first cryptographic services interface facilitates the subsequent processing of said failed request to another operating environment in the event the request is not processed or not processed correctly.

15. The cryptographic system recited in claim 13 wherein said request comprises a function call to perform cryptographic services, information or data that requires cryptographic processing, and information about the requestor.

16. The cryptographic system recited in claim 13, wherein said cryptographic services comprise at least one of encryption, decryption, digital signing, verification, message digest creation, and random number generation.

17. The system recited in claim 16, wherein said first operating environment is UNISYS MCP running on a CLEARPATH HMP/NX mainframe computer system, and wherein said alternate operating environment is WINDOWS NT running on Intel-based server within the CLEARPATH HMP/NX computer system.

18. The system recited in 17, wherein said communication between said first operating environment and said second operating environments is realized through the creation and initialization of secure communication dialogs operating via the Virtual Transport Layer (VTL).

19. In a computing system having a mainframe computer running a first operating environment and a plurality of computer servers running operating environments different from said first operating environment, a method to provide cryptography for

said computing system comprising the steps of:

(a) providing a first cryptographic services interface in said first operating environment, said cryptographic services interface receiving a plurality of requests for cryptographic services from computing applications local to said first operating environment;

(b) establishing communications with operating environments of said computer servers over a secure communications interface, such that said first cryptographic services interface has information about the availability of operating environments of said computer servers having cryptography services and the type of cryptographic services;

(c) providing a second cryptographic services interface on at least one of said computer servers to receive requests from said first cryptographic services interface and to process said received requests to distribute said requests to said cryptographic services;

(d) providing cryptographic services located in said operating environments of said computer servers that are capable of performing cryptographic functions;

(e) distributing requests to cryptographic services of said operating environments of said computer servers to perform cryptographic processing;

(f) monitoring and storing information about cryptographic processing of cryptographic services such that if cryptographic processing fails or malfunctions in a given operating environment, this information is passed back to the application so that the application can decide whether to request another session and resubmit the request or fail the request; and

(g) communicating processed requests back to said second cryptographic services interface, wherein said second cryptographic services interface communicates said processed requests to said first operating environment via said first cryptographic services interface and said first operating environment communicates said processed requests to said computing applications.

20. The method recited in claim 19, wherein said communications between said first operating environment and said operating environments of said computer servers is

realized through the creation and initialization of communication dialogs operating in accordance with the TCP/IP protocol.

21. The method recited in claim 20, wherein said requests comprise a function call to perform cryptographic services, information or data requiring cryptography, and information about the requestor.

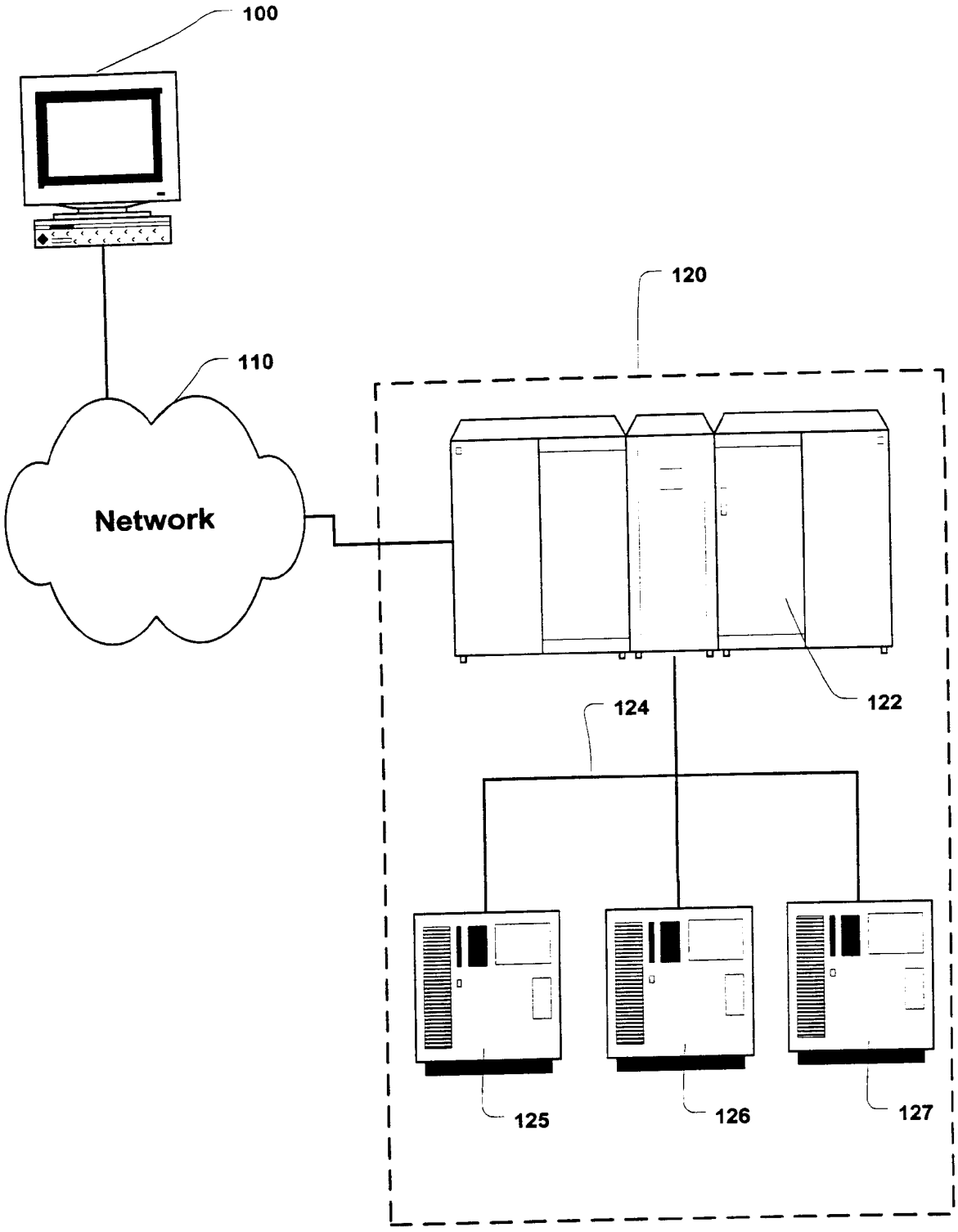

Figure 1

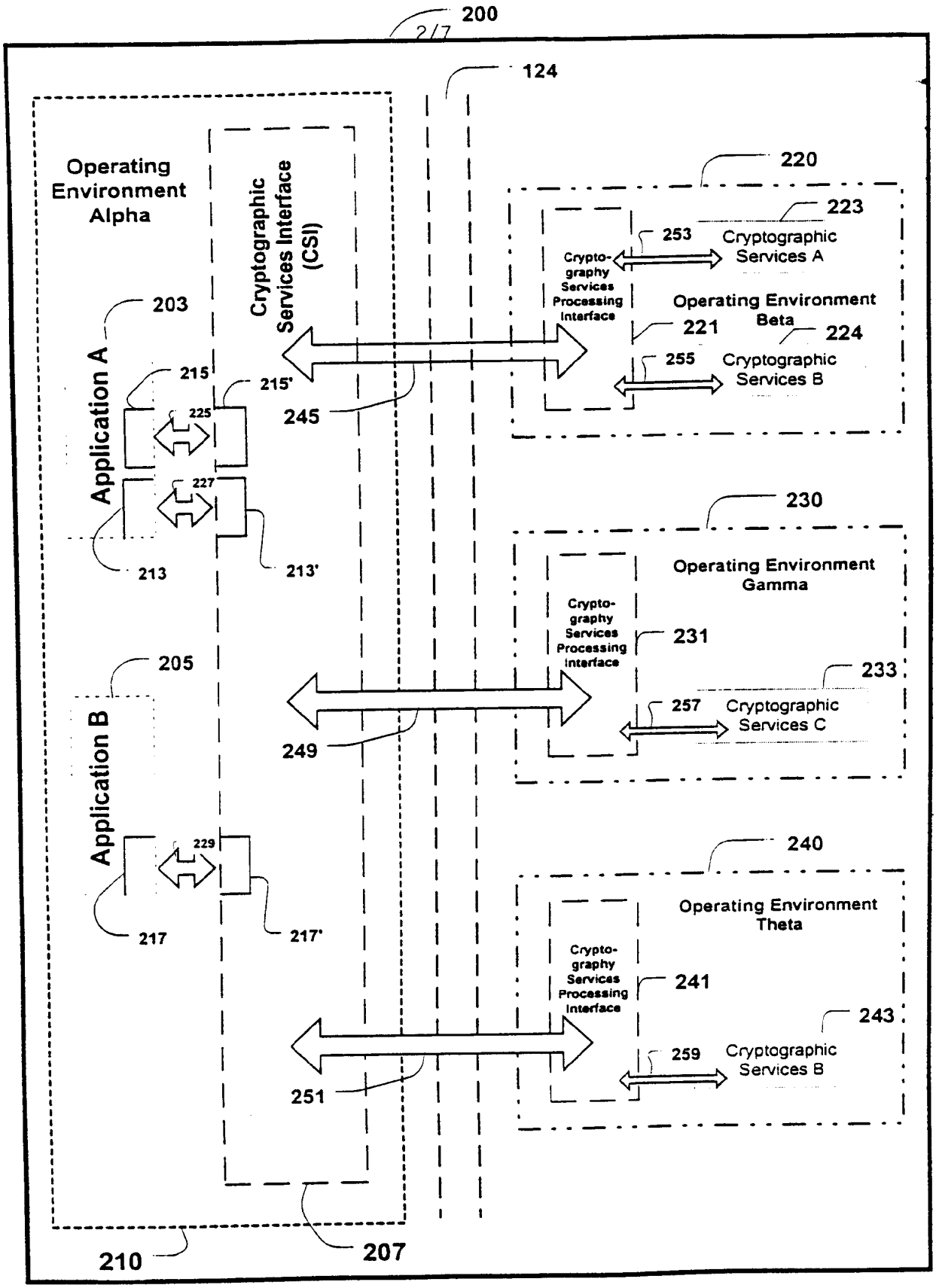
200
124
Operating Environment Alpha
Cryptographic Services Interface (CSI)
220
223
253
Cryptographic Services A
Crypto-graphy Services Processing Interface
Operating Environment Beta
221
224
255
Cryptographic Services B
203
Application A
215
215'
225
227
245
213
213'
230
Operating Environment Gamma
Crypto-graphy Services Processing Interface
231
233
257
Cryptographic Services C
205
Application B
249
229
240
Operating Environment Theta
217
217'
Crypto-graphy Services Processing Interface
241
243
259
Cryptographic Services B
251
210
207

Figure 2

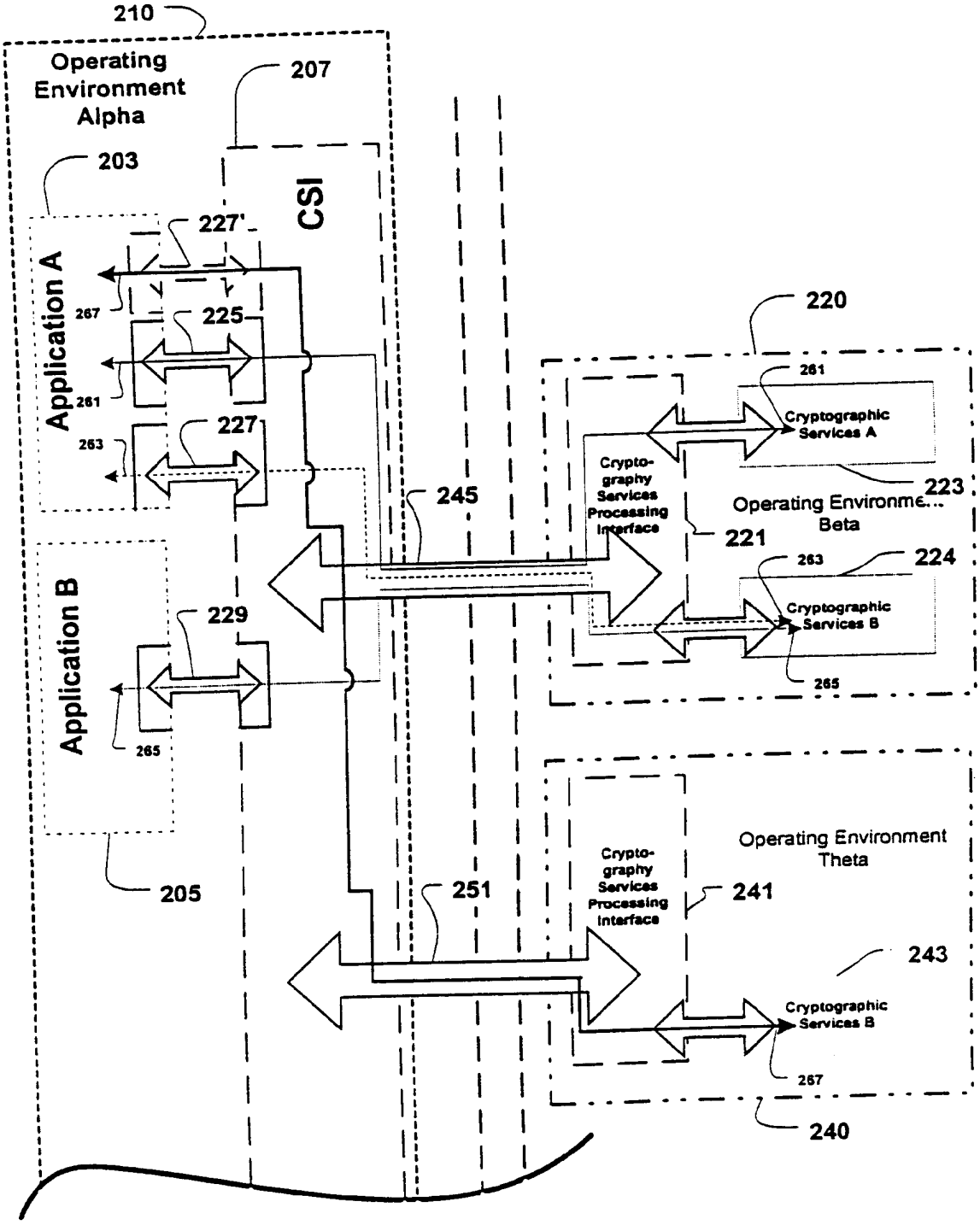
210
Operating Environment Alpha
207
203
CSI
227'
Application A
267
225
261
227
263
220
261
Cryptographic Services A
Crypto-graphy Services Processing Interface
245
221
223
Operating Environme... Beta
263
224
Cryptographic Services B
265
229
Application B
265
205
251
Crypto-graphy Services Processing Interface
241
Operating Environment Theta
243
Cryptographic Services B
267
240

Figure 2a

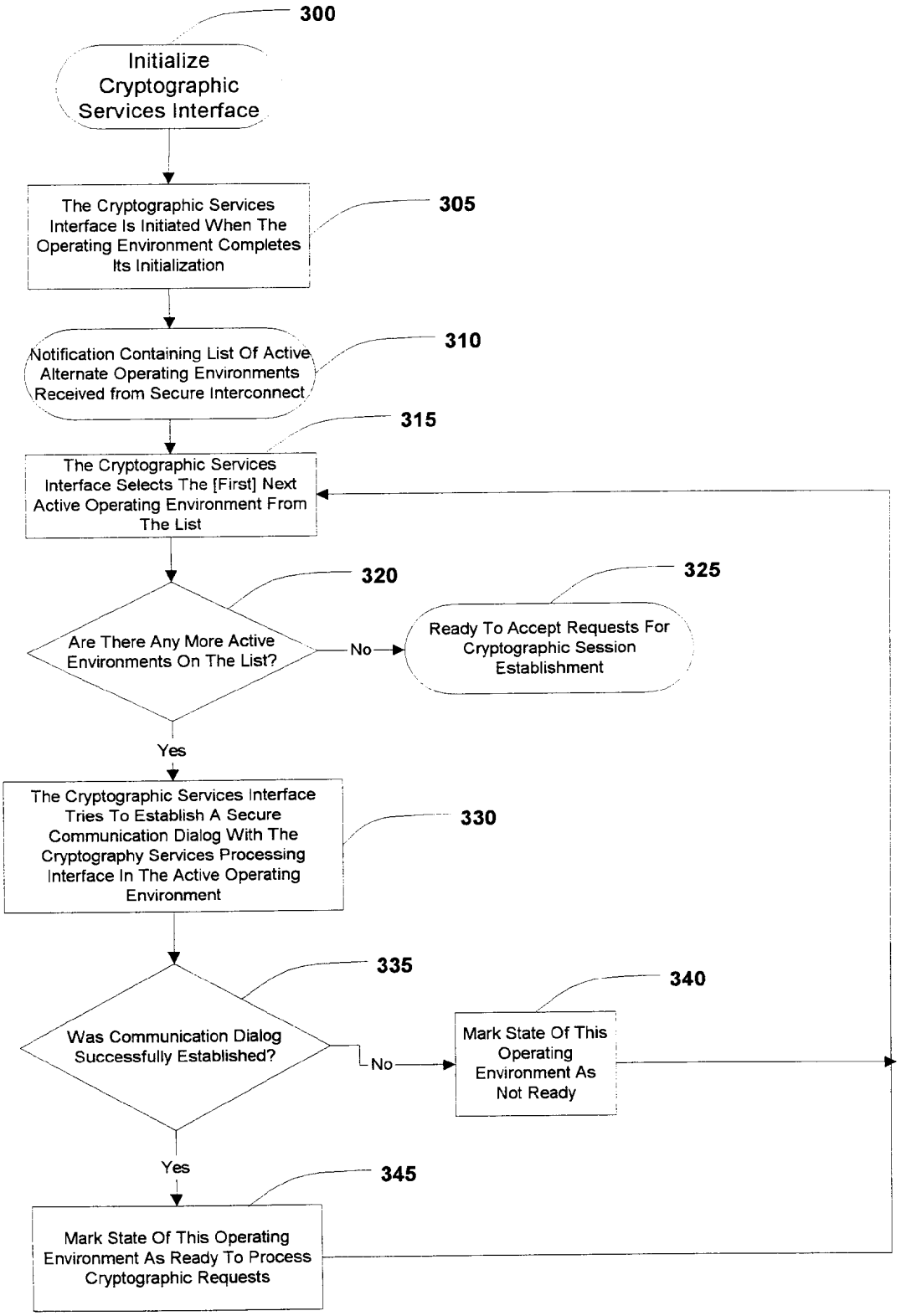
300
Initialize Cryptographic Services Interface
The Cryptographic Services Interface Is Initiated When The Operating Environment Completes Its Initialization
305
Notification Containing List Of Active Alternate Operating Environments Received from Secure Interconnect
310
The Cryptographic Services Interface Selects The [First] Next Active Operating Environment From The List
315
Are There Any More Active Environments On The List?
320
No
Ready To Accept Requests For Cryptographic Session Establishment
325
Yes
The Cryptographic Services Interface Tries To Establish A Secure Communication Dialog With The Cryptography Services Processing Interface In The Active Operating Environment
330
Was Communication Dialog Successfully Established?
335
No
Mark State Of This Operating Environment As Not Ready
340
Yes
Mark State Of This Operating Environment As Ready To Process Cryptographic Requests
345

Figure 3

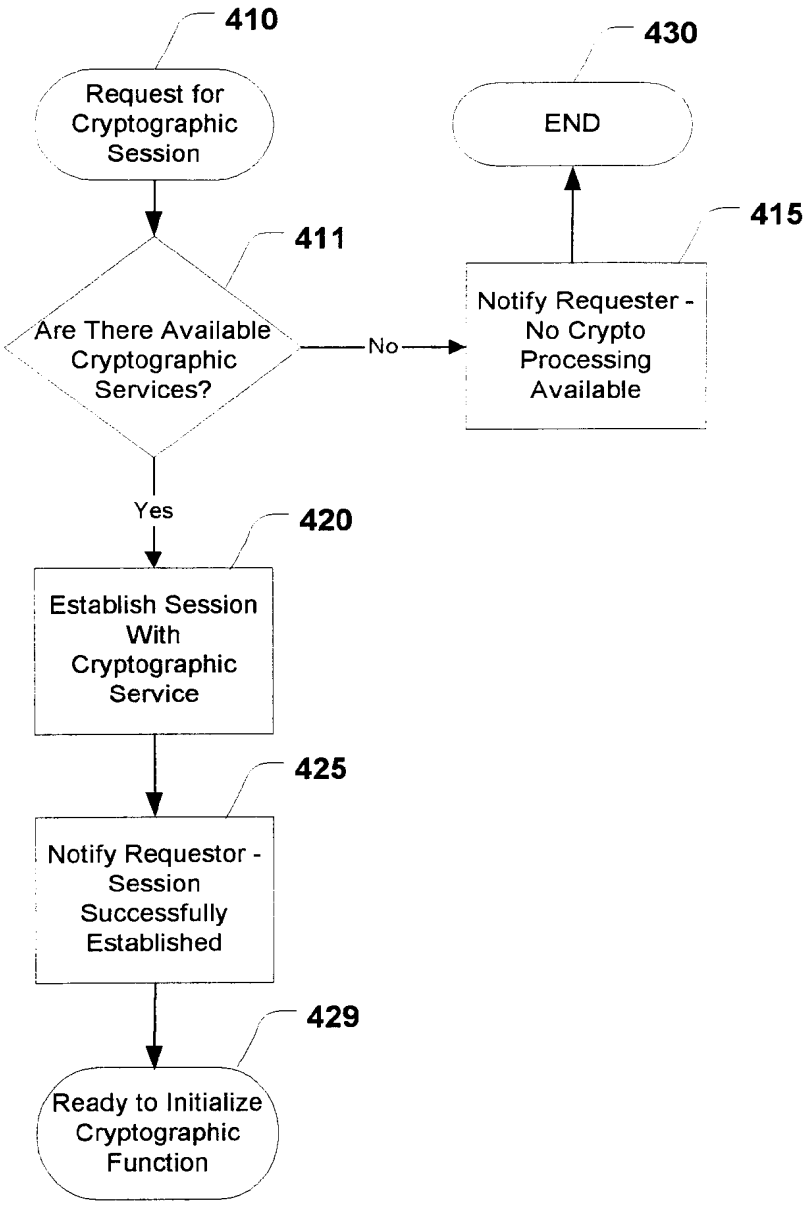
410
Request for Cryptographic Session
411
Are There Available Cryptographic Services?
No
430
END
415
Notify Requester - No Crypto Processing Available
Yes
420
Establish Session With Cryptographic Service
425
Notify Requestor - Session Successfully Established
429
Ready to Initialize Cryptographic Function

Figure 4

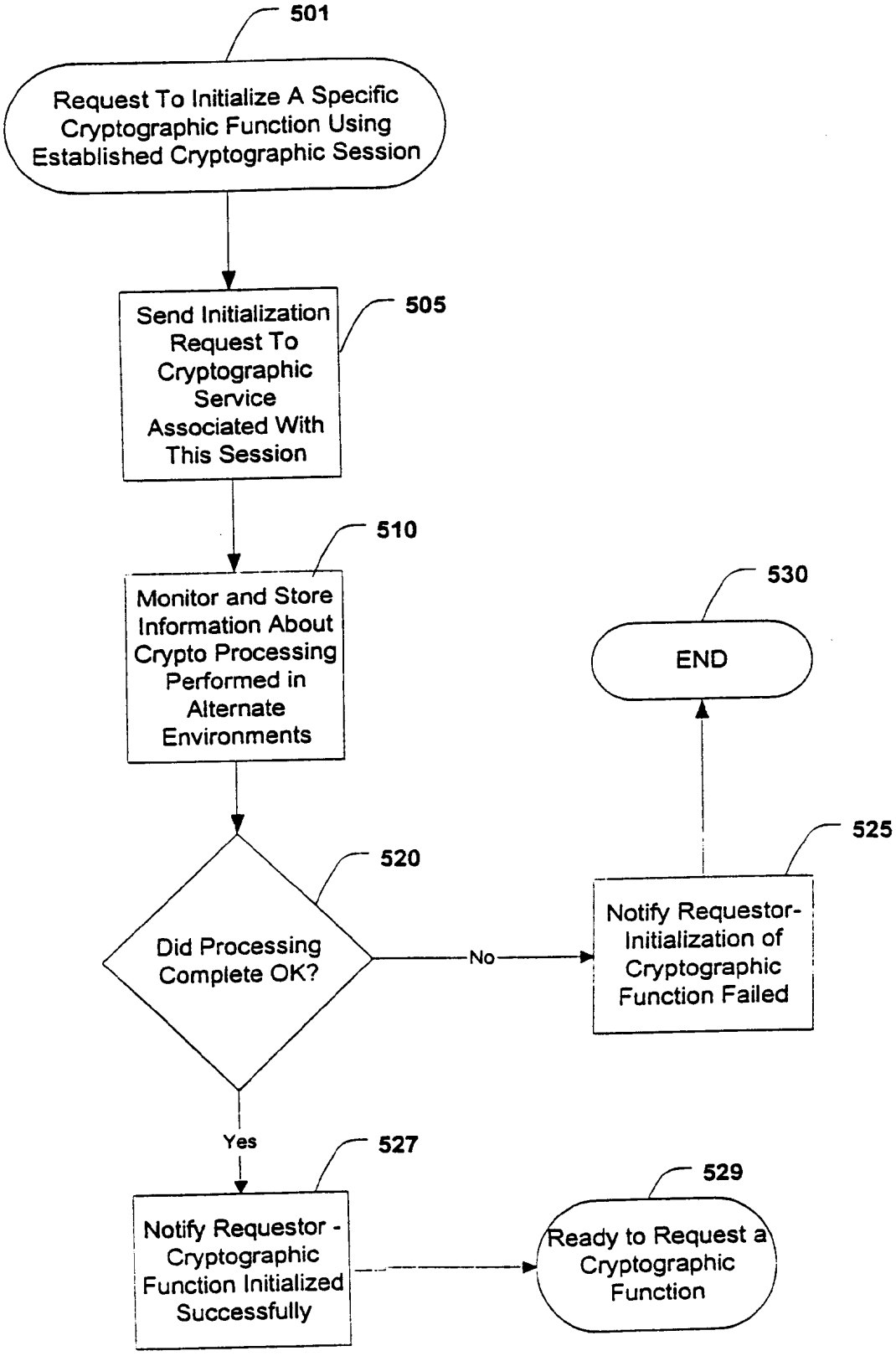
501
Request To Initialize A Specific Cryptographic Function Using Established Cryptographic Session
Send Initialization Request To Cryptographic Service Associated With This Session
505
510
Monitor and Store Information About Crypto Processing Performed in Alternate Environments
530
END
525
520
Did Processing Complete OK?
No
Notify Requestor-Initialization of Cryptographic Function Failed
Yes
527
529
Notify Requestor - Cryptographic Function Initialized Successfully
Ready to Request a Cryptographic Function

Figure 5

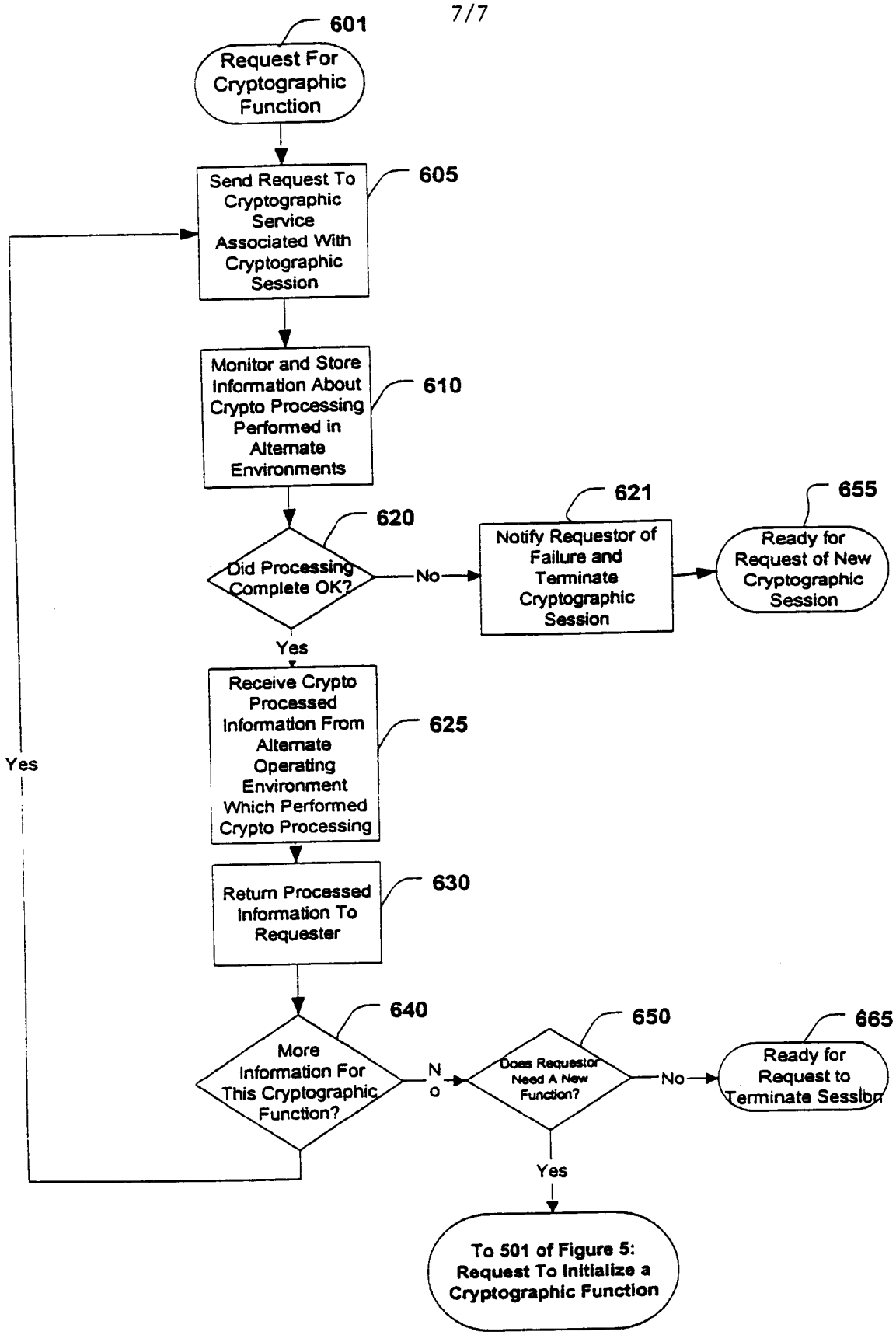
601
Request For Cryptographic Function
605
Send Request To Cryptographic Service Associated With Cryptographic Session
610
Monitor and Store Information About Crypto Processing Performed in Alternate Environments
620
Did Processing Complete OK?
No
621
Notify Requestor of Failure and Terminate Cryptographic Session
655
Ready for Request of New Cryptographic Session
Yes
625
Receive Crypto Processed Information From Alternate Operating Environment Which Performed Crypto Processing
630
Return Processed Information To Requester
640
More Information For This Cryptographic Function?
No
650
Does Requestor Need A New Function?
No
665
Ready for Request to Terminate Session
Yes
Yes
To 501 of Figure 5: Request To Initialize a Cryptographic Function

Figure 6